IN THE SPECIFICATION

Please modify the specification of the present application as follows:

Please replace the paragraph starting at page 3 line 26 with the following paragraph:

As a specific example, a permission setting for a file of "110,100,000" allows the Unix operating system to grant read and write access to user and user processes having the user identity (i.e., the user or owner) associated with that file, but disallows execute access. In this example, the operating system might deny execute access since the file might be data rather that an executable program. This permission setting allows ~~also~~ the operating system to grant read access to users and user processes that have a group identity that is the same as the group identity associated with the file, but disallows write or execute access for users or user processes that have group identities within the group associated with the file. Finally, this permission setting disallows read, write and execute access to all other users or user processes within the computer system which attempt to access the file in any manner. This example set of permissions thus provides a rather secure level of access to the file since the operating system provides only the user who owns the file (or user processes created by that user) the ability to read and write to the file, and only members of the group associated with the file (or processes that they create) are provided with read-only access to the file.

Please replace the paragraph starting at page 6 line 15 with the following paragraph:

The ~~To~~ present invention significantly overcomes many of the aforementioned drawbacks of conventional authorization and access control mechanisms. The system of this invention provides a flexible authorization

system providing robust access control to resources in a computing system environment. The authorization system is typically embodied within a computer system configured to provide access control to one or more resources such as data or portions of a data storage system, though access control to any resource can be provided by this invention.

Please replace the paragraph starting at page 7 line 26 with the following paragraph:

If the disregard instruction is conditional, then it ~~if~~ might cause further rule processing to disregard (i.e., to not process) certain rule operations, while allowing other remaining rule operations in the selected set of rule (initially selected by the filter operation(s) ) to be processed. As an example, a disregard instruction might instruct a rule engine (to be explained) that performs rule processing to disregard any further rule operations relating to payroll data. As rule processing continues, the rule engine would thus not process rule operations in other rules within the selected set of rules that have an effect on payroll data.

Please replace the paragraph starting at page 19 line 10 with the following paragraph:

Fig. 1 illustrates an example computing system environment 100 in which the present invention can be applied to provide authorization and access control to various computing system resources. In this example, the computing system environment 100 represents a typical corporate computer network and includes departments 120 through 124 that each have various computer users using one or more computing systems coupled to each other via a computer network 110. The departments in this example include a systems management department 120, an engineering department 121, an accounting department 122, a sales department 123 and a CEO/executive (i.e., management) department 124.

Computer users who are ~~a~~ members of a particular department might be stored in a database (not shown in this figure), for example. The computing environment 100 also includes a resource server 200, which in this example is a workstation computer system (being operated by a systems manager 120) configured to provide access to (i.e., to serve) data stored within the data storage systems 160-1 through 160-N to the various computer systems within the departments 120 through 124. In this example, the resources to which the system of the invention governs authorization are the data storage systems 160-1 through 160-N, which can be, for example, high-capacity data storage systems such as one or more SYMMETRIX ~~Symmetrix~~ data storage systems manufactured by EMC Corporation of Hopkinton, Massachusetts. SYMMETRIX ~~Symmetrix~~ is a registered trademark of EMC Corporation. Within the resource server 200, a role/rule-based authorization system 300, 350 configured according to the invention provides an authorization and access control mechanism to govern access on behalf of computer users (i.e., people in the various departments 120 through 124) to resources such as data, files, databases, volumes, partitions and the like stored within the data storage systems 160-1 through 160-N (the resources).

Please replace the paragraph starting at page 30 line 29 with the following paragraph:

Fig. 4 illustrates an example portion of a managed object 360 that represents the data storage system 160-1, as contained within the managed object database 350-5. As shown, the managed object 360 includes various data fields 362 through 370 that store information and attributes related to the object represented. The object label field 362 identifies the actual resource which this object 360 represents, which in this example is a SYMMETRIX ~~Symmetrix~~ data storage system 160-1 manufactured by EMC Corporation of Hopkinton, Massachusetts.

Please replace the paragraph starting at page 32 line 15 with the following paragraph:

A commercial database package such as ORACLE ~~Oracle~~ (trademarked and manufactured by Oracle Corporation) or an object-oriented database can be used to maintain the database of managed resources 350-3 (as well as other databases 350), or each managed object (e.g., 360) can be maintained as an independent data structure in an object-oriented or other programming environment such as those provided by the Java or C++ computing language and software development environments.

Please replace the paragraph starting at page 48 line 3 with the following paragraph:

In step 421, if the access request is a query access request 301-2, then the query engine 320 processes step 423 to apply at least one filter operation, using the identity of the resource and/or the role identity of the requestor and/or the a type of access being requested, for rules in the master set of rules 350-4 to produce a list of rules which match the filter operation. Next, in step 424, the query engine 320 provides an indication of the authorization state of the role-rule-based access control system 300 based on the list of rules as related to the identity of the resource and/or the role identity of the requestor and/or the a type of access being requested. In this manner, a user can query the access control system 300 to determine, for example, what rules in the master set of rules 350-4 might be applied in a particular access control scenario (i.e., based on the values for the REQUESTOR, ACCESS and RESOURCE specified in an access request 301).